Optimal unambiguous discrimination of two subspaces as a case in mixed state discrimination

János A. Bergou,[1] Edgar Feldman,[2] and Mark Hillery[1]

[1] *Department of Physics and Astronomy, Hunter College of the City University of New York, 695 Park Avenue, New York, NY 10021*

[2] *Department of Mathematics, Graduate Center of the City University of New York, 365 Fifth Avenue, New York, NY 10016*

(Dated: February 1, 2008)

We show how to optimally unambiguously discriminate between two subspaces of a Hilbert space. In particular we suppose that we are given a quantum system in either the state $|\psi_1\rangle$, where $|\psi_1\rangle$ can be any state in the subspace S_1, or $|\psi_2\rangle$, where $|\psi_2\rangle$ can be any state in the subspace S_2, and our task is to determine in which of the subspaces the state of our quantum system lies. We do not want to make any error, which means that our procedure will sometimes fail if the subspaces are not orthogonal. This is a special case of the unambiguous discrimination of mixed states. We present the POVM that solves this problem and several applications of this procedure, including the discrimination of multipartite states without classical communication.

PACS numbers: 03.67.-a,03.65.Bz,42.50.-p

I. INTRODUCTION

The discrimination of quantum states is an area that has received considerable attention. For a recent review see [1], for example. Pure state discrimination has proven to be useful for both quantum cryptography and for quantum algorithms [2, 3]. The basic protocol is the following. One has a list of possible quantum states, and one is presented with a system that is guaranteed to be in one of them. Our task is to determine which. If the states are not orthogonal, they cannot be discriminated perfectly, and it is necessary to specify what kind of strategy we wish to use. One possibility is minimum error discrimination [4]. In this procedure, we always specify a state, but, because the states are not orthogonal, there is some chance that we will make a mistake. Minimum-error procedures minimize the chance of making a mistake. Another alternative is unambiguous discrimination. This procedure never makes a mistake, but it can sometimes fail. If the list of states contains N possibilities, then this procedure has $N + 1$ possible outputs, one for each of the states on list plus a failure output. If we receive an output that specifies one of the states, then we know what the state of our system was, and if we receive the failure output, then we have no idea what it was. An optimum unambiguous procedure is one that minimizes the probability of receiving the failure output. We shall be considering unambiguous discrimination here.

The problem of optimal unambiguous discrimination between two pure quantum states was solved by Ivanovic, Dieks and Peres [5, 6, 7]. They assumed that each of the two states were equally probable. The case in which they are not was treated by Jaeger and Shimony [8] (for a somewhat simpler derivation of their result see [9]). The case of more than two pure states is not simple and has been considered by a number of authors. There are a few general results, but explicit procedures are available only for special cases [10, 11]. One important result is that for unambiguous discrimination to be possible, the states on the list must be linearly independent [12]. There are also lower bounds on the failure probability [13].

The discrimination of two mixed states has only been considered more recently. Before we cite the previous results it will be useful to introduce some terminology at this point. The support S_j of the density operator ρ_j, describing a quantum state, is the subspace of the entire Hilbert space $\mathcal{H}$ spanned by the eigenvectors of ρ_j belonging to nonzero eigenvalues (for $j = 1, 2$). The rank of the density operator is equal to the dimension of its support. The subspace orthogonal to its support, $\bar{S}_j$, is the kernel of the density operator ρ_j such that $\mathcal{H} = S_j \oplus \bar{S}_j$. We shall denote the projector onto S_j by P_j and the projector onto $\bar{S}_j$ by $\bar{P}_j$. Equipped with these definitions we can now make the following general statement. For two mixed quantum states unambiguous discrimination is possible with a finite probability of success if and only if the supports of their density operators are not identical. Indeed, in such a case the kernel of at least one of them is not empty and a projective measurement along this kernel unambiguously identifies the other state. On the other hand, if the supports are identical, then so are their kernels, and there is no direction in $\mathcal{H}$ that could unambiguously identify at least one of the density operators.

We can now return to a listing of earlier results. The POVM for unambiguously discriminating between a pure state and a rank two mixed state was derived in [14] and subsequently generalized to the case of unambiguously discriminating a pure state from any mixed state [3]. Lower bounds on the failure probability for the unambiguous discrimination of two mixed states were derived by Rudolph *et al.* [15] and for an arbitrary number of mixed states by Feng *et al.* [16]. Raynal *et al.* [17] proved two theorems that make it possible to reduce the problem of unambiguously discriminating between two arbitrary

mixed states of rank k_1 and k_2 to the discrimination of two states of the same rank, $k \leq min(k_1, k_2)$, in a $2k$-dimensional space. Building on the results of [15] and [16], Herzog and Bergou [18] found explicit solutions for some special cases along with necessary conditions for the saturation of the lower bound. In particular, these results showed that unlike in the case of two pure states whether or not the lower bound can be attained depends not only on the value of the prior probabilty of the states but also on their structure. There are mixed states for which the lower bound can not be reached for any value of the prior probability. In [19] the optimal measurement operators were constructed explicitly for some special cases.

In this paper we shall consider the unambiguous discrimination between two subspaces. What this means is the following. A state is chosen from one of two subspaces, and we wish to determine to which of the subspaces the state belongs. Within each subspace each state is equally likely, though one subspace may be more likely than the other. One place in which this type of problem has arisen is in the consideration of programmable discriminators [20]. In this case, one is given three qubits, the first two are arbitrary but the third is guaranteed to be identical to either the first or the second qubit, and the problem is to determine which two qubits are identical. The problem can be solved by realizing that one is, in fact, discriminating between two subspaces, the first being the subspace of three-qubit states that is symmetric in the first and third qubits, and the second being the subspace that is symmetric in the second and third qubits.

Subspace discrimination is a special case of the discrimination of two mixed states; in this case the density matrices are just proportional to the projection operators onto the subspaces. Making use of the results of Raynal *et al.* [17], we can restrict our attention to the case of two subspaces of dimension k in a $2k$ dimensional space. In particular, let S_1, and S_2 be k-dimensional subspaces of the entire Hilbert space, $\mathcal{H}$, which has dimension $2k$. We can assume that the intersection of S_1 and S_2 is just the zero vector, a situation which we henceforth refer to as general position. We assume that $\rho_1 = (1/k)P_1$ occurs with probability η, and $\rho_2 = (1/k)P_2$ occurs with probability $1-\eta$, where P_j is the projection onto S_j, for $j = 1, 2$. The POVM that distinguishes them has three elements, Π_1, Π_2, and $\Pi_0 = I - \Pi_1 - \Pi_2$, all of which are positive operators. The probability of identifying ρ_j if we are given ρ_j is $p_j = \mathrm{Tr}(\rho_j \Pi_j)$, and the probability of failing to identify it is $q_j = \mathrm{Tr}(\rho_j \Pi_0)$, for $j = 1, 2$. The condition that a state never be misidentified implies that $\Pi_1 \rho_2 = \Pi_2 \rho_1 = 0$. The average failure probability is

$$Q = \eta q_1 + (1-\eta) q_2 \ , \tag{1.1}$$

and our object is to find, for a given η, a POVM that minimizes Q. From the results in [15] and [16], we have that

$$Q \geq 2\sqrt{\eta(1-\eta)} F(\rho_1, \rho_2) \ , \tag{1.2}$$

where the fidelity between the two density matrices is given by

$$F(\rho_1, \rho_2) = \mathrm{Tr}((\rho_1^{1/2} \rho_2 \rho_1^{1/2})^{1/2}) \ . \tag{1.3}$$

The conditions, under which this bound can be saturated, have been investigated in [18]. In [19] the optimum POVM has been given explicitly for certain special cases. As we shall see, unlike for the case of two pure states, this bound cannot always be reached for two mixed states, in agreement with [18]. The optimal measurement procedure depends on the value of η, a feature it has in common with the procedure for discriminating two pure states. For two pure states there is always a range of η where equality in (1.2) can be reached. In the case of two mixed states, however, the optimal measurement procedure also depends on the structure of the two density operators, a distinctive feature that has no equivalent in the case of two pure states. For η near 0 or 1 the optimal measurements are projective ones. In the intermediate regime, the optimal measurements are intermittently POVM's or projective measurements and, in general, their failure probability is higher than the fidelity bound (1.2). Only under very special conditions shall we find that the fidelity bound can be saturated.

The main technical device that we shall use to find the optimal measurements is that of Jordan bases. These bases take the following form. The states $|\psi_1\rangle, \ldots |\psi_k\rangle$ form an orthonormal basis for S_1, $|\psi_{k+1}\rangle, \ldots |\psi_{2k}\rangle$ form an orthonormal basis for S_2, and, in addition these states have the property that

$$\langle \psi_i | \psi_{k+j} \rangle = \delta_{ij} \cos\theta_i, \tag{1.4}$$

where $\cos\theta_1 \geq \cos\theta_2 \geq \ldots \cos\theta_k$, and $1 \leq i, j \leq k$. The states $|\psi_1\rangle, \ldots, |\psi_k\rangle$ and $|\psi_{k+1}\rangle, \ldots, |\psi_{2k}\rangle$ are called Jordan bases and the angles θ_i are called the Jordan angles. Bases satisfying these conditions can be constructed for any two subspaces [21]. Note that the basis vectors $|\psi_i\rangle$ and $|\psi_{k+i}\rangle$ are eigenvectors of the operators $P_1 P_2 P_1$ and $P_2 P_1 P_2$, respectively, where

$$\begin{aligned} P_1 P_2 P_1 |\psi_i\rangle &= \cos^2\theta_i |\psi_i\rangle \ , \\ P_2 P_1 P_2 |\psi_{k+i}\rangle &= \cos^2\theta_i |\psi_{k+i}\rangle \ , \end{aligned} \tag{1.5}$$

where $1 \leq i \leq k$.

The paper is organized as follows. Sec. II is devoted to the derivation of the general results. Besides giving the general theory for distinguishing two k dimensional subspaces in a $2k$ dimensional Hilbert space, these results also hold for a rather general class of density operators, so they are directly relevant to the problem of optimal unambiguous discrimination between two mixed states. In Sec. III we present some possible applications of the results. Finally, in Sec. IV we give a brief summary and outlook for future research.

II. DISTINGUISHING SUBSPACES AND ITS RELATION TO THE DISCRIMINATION OF MIXED STATES

We shall actually solve a somewhat more general problem than the discrimination of two subspaces. Let S_1 and S_2 be k dimensional subspaces of a $2k$ dimensional complex Hilbert space $\mathcal{H}$ which are in general position, as discussed in the introduction, and let $\{|\psi_1\rangle, \ldots, |\psi_k\rangle\}$ and $\{|\psi_{k+1}\rangle, \ldots, |\psi_{2k}\rangle\}$ be Jordan bases associated to these subspaces. Consider the two density matrices

$$\begin{aligned} \rho_1 &= \sum_{i=1}^{k} \alpha_i |\psi_i\rangle\langle\psi_i| \ , \\ \rho_2 &= \sum_{i=1}^{k} \beta_i |\psi_{i+k}\rangle\langle\psi_{i+k}| \ , \end{aligned} \tag{2.1}$$

where $\alpha_i > 0$, $\sum_i \alpha_i = 1$, $\beta_i > 0$, and $\sum_i \beta_i = 1$. Clearly, ρ_1 has support in S_1 and ρ_2 has support in S_2. In this case the orthonormal frames for the density matrices given by the spectral theorem coincide with the Jordan frames of the supports. If

$$\begin{aligned} \rho_1 &= (1/k) \sum_{i=1}^{k} |\psi_i\rangle\langle\psi_i| \\ \rho_2 &= (1/k) \sum_{i=1}^{k} |\psi_{i+k}\rangle\langle\psi_{i+k}|, \end{aligned} \tag{2.2}$$

we say that ρ_1 and ρ_2 are uniformly mixed states, and discriminating between uniformly mixed states corresponds to the case of discriminating between the subspaces S_1 and S_2. Inserting the weights α_i and β_i will allow us to address several issues in the general theory of mixed state discrimination.

We will now construct an optimal POVM to unambiguously discriminate between ρ_1 and ρ_2. The POVM elements are Π_1, Π_2 and $\Pi_0 = I - \Pi_1 - \Pi_2$ with the properties as discussed in the introduction. Π_1 and Π_2 are self adjoint operators supported on $\bar{S}_2$ and $\bar{S}_1$, respectively. In order for them to form an optimal POVM they must be positive and, crucially, the rank of Π_0 must not exceed k [17]. We wish to choose Π_1 and Π_2 so that the expression $P(\eta) = \eta \mathrm{Tr}(\Pi_1\rho_1) + (1-\eta)\mathrm{Tr}(\Pi_2\rho_2)$ is maximized. This is the same as minimizing the average failure probability $Q(\eta) = \eta \mathrm{Tr}(\Pi_0\rho_1) + (1-\eta)\mathrm{Tr}(\Pi_0\rho_2)$ that was introduced in (1.1).

Let T_i be the linear subspace spanned by $|\psi_i\rangle$ and $|\psi_{i+k}\rangle$. The T_i's, with $1 \le i \le k$, are mutually orthogonal, two dimensional subspaces, which are invariant under both ρ_1 and ρ_2. Let us define states $|z_i\rangle$ and $|y_i\rangle$ as

$$\begin{aligned} |\psi_i\rangle &= \sin\theta_i |z_i\rangle + \cos\theta_i |\psi_{i+k}\rangle \\ |\psi_{i+k}\rangle &= \sin\theta_i |y_i\rangle + \cos\theta_i |\psi_i\rangle, \end{aligned} \tag{2.3}$$

where $|z_i\rangle$ ($|y_i\rangle$) is the orthogonal complement of $|\psi_{i+k}\rangle$ ($|\psi_i\rangle$) in T_i. Furthermore $\{|z_1\rangle, \ldots, |z_k\rangle\}$ forms an orthonormal basis for $\bar{S}_2$, and $\{|y_i\rangle, \ldots, |y_k\rangle\}$ forms an orthonormal basis for $\bar{S}_1$.

If we write $\Pi_1 = \sum_{i,j=1}^{k} a_{ij} |z_i\rangle\langle z_j|$ and $\Pi_2 = \sum_{i.j=1}^{k} b_{ij} |y_i\rangle\langle y_j|$, then

$$p_1 = \mathrm{Tr}(\Pi_1\rho_1) = \sum_{i=1}^{k} a_{ii}\alpha_i \sin^2\theta_i \ , \tag{2.4}$$

and

$$p_2 = \mathrm{Tr}(\Pi_2\rho_2) = \sum_{i=1}^{k} b_{ii}\beta_i \sin^2\theta_i \ . \tag{2.5}$$

These equations do not depend upon the off-diagonal terms of Π_1 and Π_2. If Π_1 and Π_2 are to be elements of a POVM they must be positive so $a_{ii}, b_{ii} \ge 0$ is a minimum requirement. The presence of off-diagonal elements imposes additional restrictions on the diagonal elements if we wish to ensure positivity. Since the off-diagonal elements do not play a role in p_1 and p_2, it suffices to search for our optimal POVM among the diagonal operators.

Let $\bar{p}_i = \langle\psi_i|\Pi_1|\psi_i\rangle$ and $\bar{p}_{i+k} = \langle\psi_{i+k}|\Pi_2|\psi_{i+k}\rangle$ be the individual success probabilities of the Jordan basis states for $1 \le i \le k$. Let $\bar{q}_i = \langle\psi_i|\Pi_0|\psi_i\rangle$ and $\bar{q}_{i+k} = \langle\psi_{i+k}|\Pi_0|\psi_{i+k}\rangle$ be the individual failure probabilities of the Jordan basis states for $1 \le i \le k$. Here we introduced the overbar notation in order to distinguish the partial success and failure probabilities, $\bar{p}_i$ and $\bar{q}_i$, of $|\psi_i\rangle$ from the total success and failure probabilities, p_j and q_j, of ρ_j for $i \le k$ and $j = 1, 2$. Obviously, $\bar{p}_i + \bar{q}_i = 1$ holds. We can then express the POVM operators as $\Pi_1 = \sum_{i=1}^{k} \Pi_{1,i}$ and $\Pi_2 = \sum_{i=1}^{k} \Pi_{2,i}$ where

$$\Pi_{1,i} = \frac{1-\bar{q}_i}{\sin^2\theta_i} |z_i\rangle\langle z_i|, \tag{2.6}$$

and

$$\Pi_{2,i} = \frac{1-\bar{q}_{i+k}}{\sin^2\theta_i} |y_i\rangle\langle y_i|. \tag{2.7}$$

We can also set $\Pi_0 = \sum_{i=1}^{k} \Pi_{0,i}$, where $\Pi_{0,i} = I_{T_i} - \Pi_{1,i} - \Pi_{2,i}$, and I_{T_i} is the identity in T_i.

We now need to determine the values of $\bar{q}_i$ and $\bar{q}_{i+k}$. This can be done by noticing that what we have done is to reduce our problem to k problems of optimally discriminating two vectors, in particular the vector $|\psi_i\rangle$ from the vector $|\psi_{i+k}\rangle$ in T_i. In more detail the situation is the following. In our overall ensemble, with ρ_1 occurring with probability η and ρ_2 with probability $1-\eta$, the probability of occurrence for $|\psi_i\rangle$ is $\eta\alpha_i$ and the probability for the occurrence of $|\psi_{i+k}\rangle$ is $(1-\eta)\beta_i$. Therefore, the probability for the occurrence of a vector in T_i is just the sum of these probabilities,

$$p(T_i) = \eta\alpha_i + (1-\eta)\beta_i \tag{2.8}$$

Now, the probability that $|\psi_i\rangle$ occurs given that T_i has ocurred is $p(i|T_i) = \eta\alpha_i / p(T_i)$ and the probability that

$|\psi_{i+k}\rangle$ occurs given that T_i has occurred is $p(i+k|T_i) = (1-\eta)\beta_i/p(T_i)$. Consequently, in T_i we want to unambiguously discriminate $|\psi_i\rangle$ occurring with probability $p(i|T_i)$ and $|\psi_{i+k}\rangle$ occuring with probability $p(i+k|T_i)$ so as to minimize the failure probability

$$Q_i(\eta) = p(i|T_i)\bar{q}_i + p(i+k|T_i)\bar{q}_{i+k}. \tag{2.9}$$

This problem was first solved by Jaeger and Shimony [8], (a somewhat simpler solution is given in [9]), and we can now make use of that solution. Let

$$I_i = \left[\frac{\beta_i \cos^2\theta_i}{\alpha_i + \beta_i\cos^2\theta_i}, \frac{\beta_i}{\beta_i + \alpha_i\cos^2\theta_i}\right] = [c_i, d_i] \tag{2.10}$$

and, in addition, let

$$\bar{q}_i^{opt}(\eta) = \sqrt{\frac{(1-\eta)\beta_i}{\eta\alpha_i}}\cos\theta_i \ . \tag{2.11}$$

For a given η, the value of $\bar{q}_i$ which minimizes $Q_i(\eta)$ is

$$q_i(\eta) = \begin{cases} 1 & \eta \le c_i \\ \bar{q}_i^{opt}(\eta) & \text{if } \eta \text{ is in } I_i \\ \cos^2\theta_i & \eta \ge d_i \end{cases} \tag{2.12}$$

and $q_{k+i}(\eta) = \cos^2\theta_i/q_i(\eta)$. Furthermore the rank of $\Pi_{0,i}$ is one, with the nonzero eigenvalue given by

$$\lambda_i = \left(\frac{\cos^2\theta_i}{\bar{q}_i} - 2\cos^2\theta_i + \bar{q}_i\right)\frac{1}{\sin^2\theta_i} \ , \tag{2.13}$$

with the corresponding eigenstate

$$|\zeta_i\rangle = \frac{\cos\theta_i(1-\bar{q}_i)}{\sin^2\theta_i}|\psi_{i+k}\rangle + \frac{\bar{q}_i - \cos^2\theta_i}{\sin^2\theta_i}|\psi_i\rangle \ . \tag{2.14}$$

This specifies the POVM within T_i.

The optimal overall failure probability can now be expressed as

$$\begin{aligned} Q^{opt} &= \sum_{i=1}^{k} Q_i^{opt} p(T_i) \\ &= \sum_{i=1}^{k} [\eta\alpha_i\bar{q}_i(\eta) + (1-\eta)\beta_i\bar{q}_{k+i}(\eta)] \ , \end{aligned} \tag{2.15}$$

where Q_i^{opt} is the failure probability that results when Eq. (2.12) is substituted into Eq. (2.9). Its explicit expression is given by

$$Q_i^{opt}p(T_i) = \begin{cases} \eta\alpha_i + (1-\eta)\beta_i\cos^2\theta_i & \text{if } \eta \le c_i \\ 2\sqrt{\eta(1-\eta)\alpha_i\beta_i}|\cos\theta_i| & \text{if } c_i \le \eta \le d_i \\ \eta\alpha_i\cos^2\theta_i + (1-\eta)\beta_i & \text{if } \eta \ge d_i \end{cases} \ . \tag{2.16}$$

The center line is the geometric mean of the two terms in either the first or the last line and, therefore, represents an absolute minimum for Q_i. We obtain the absolute possible minimum of the total failure probability if we sum the center lines for all $1 \le i \le k$. The summation yields

$$Q^{opt} = 2\sqrt{\eta(1-\eta)}\sum_{i=1}^{k}\sqrt{\alpha_i\beta_i}|\cos\theta_i| \ . \tag{2.17}$$

Clearly, this absolute minimum can only be realized if and only if the intersection of all of the intervals I_i is not empty and the operating value of η is in this intersecton.

The interpretation of this expression is straightforward. Making use of the structure of the Jordan bases, we obtain $\rho_1^{\frac{1}{2}}\rho_2\rho_1^{\frac{1}{2}} = \sum_i \alpha_i\beta_i\cos^2\theta_i|\psi_i\rangle\langle\psi_i|$, after a simple calculation. Comparing this expression with Eq. (1.3) tells us immediately that Eq. (2.17) can be cast to the form

$$Q^{opt} = 2\sqrt{\eta(1-\eta)}F(\rho_1,\rho_2) \ , \tag{2.18}$$

where $F(\rho_1,\rho_2) = \sum_i\sqrt{\alpha_i\beta_i}|\cos\theta_i|$. Here $F(\rho_1,\rho_2)$ is the fidelity between ρ_1 and ρ_2, constructively proving that the fidelity bound, Eq. (1.2), can be saturated. To obtain an explicit expression for the fidelity would be a hopeless task, in general. What made it possible here is the fact that the density operators are diagonal in the Jordan bases of their support and we could take full advantage of the ensuing Jordan structure. Furthermore, the above expression for the optimum failure probability holds only if η is an element of the intersection of all of the I_i intervals, $I_0 = \bigcap_{i=1}^{k} I_i$. I_0 may be empty, it often is. Note, however, that in the case where ρ_1 and ρ_2 are uniformly mixed states, which is the case of subspace discrimination,

$$I_i = \left[\frac{\cos^2\theta_i}{1+\cos^2\theta_i}, \frac{1}{1+\cos^2\theta_i}\right] \subseteq I_{i+1} \tag{2.19}$$

so $I_0 = I_1 \neq \emptyset$ and the fidelity result holds in the entire I_1 interval.

For the case when $k = 2$ there are only two such intervals, I_1 and I_2, and we will now give a complete classification of their intersection pattern. To this end, we first introduce a one-parameter characterization of ρ_1 and ρ_2. Let us set $\alpha_1 = \alpha$ and, consequently, $\alpha_2 = 1-\alpha$. Similarly, we set $\beta_1 = \beta$ and, consequently, $\beta_2 = 1-\beta$. We can now introduce a two-dimensional parameter plane, $\alpha\beta$, where the square in the first quadrant, bounded by $0 \le \alpha \le 1$ and $0 \le \beta \le 1$, corresponds to physically acceptable choices for mixed states. So our task is reduced to finding the regions within this square with qualitatively different overlap patterns. When $\cos^2\theta_1 > \cos^2\theta_2$, which is the convention that we adopted at the beginning, the patterns can be sorted into five categories:
i) $d_1 < c_2$, i. e. I_1 is to the left of I_2 and their intersection is empty. This happens when

$$\beta \le \bar{\beta}_1(\alpha) = \frac{\alpha\cos^2\theta_1\cos^2\theta_2}{1-\alpha(1-\cos^2\theta_1\cos^2\theta_2)} \ . \tag{2.20}$$

$\bar{\beta}_1(\alpha)$ is a hyperbola in the $\alpha\beta$ plane and it is the divider between this region and the next, when

ii) $c_1 < c_2 < d_1 < d_2$, i. e. the right end of I_1 partially overlaps with the left end of I_2 and their intersection is the overlap. This happens when

$$\beta \leq \bar{\beta}_2(\alpha) = \frac{\alpha \cos^2\theta_2}{\cos^2\theta_1 - \alpha(\cos^2\theta_1 - \cos^2\theta_2)} \ . \qquad (2.21)$$

$\bar{\beta}_2(\alpha)$ is a hyberbola in the $\alpha\beta$ plane and it is the divider between this region and the next, when
iii) $c_2 < c_1$ and $d_1 < d_2$, i. e. I_1 is inside I_2 and the intersection coincides with I_1. This happens when

$$\beta \leq \bar{\beta}_3(\alpha) = \frac{\alpha \cos^2\theta_1}{\cos^2\theta_2 + \alpha(\cos^2\theta_1 - \cos^2\theta_2)} \ . \qquad (2.22)$$

$\bar{\beta}_3(\alpha)$ is a hyberbola in the $\alpha\beta$ plane and it is the divider between this region and the next, when
iv) $c_1 < c_2 < d_2 < d_1$, i. e. the left end of I_1 partially overlaps with the right end of I_2 and the intersection is the overlap. This happens when

$$\beta \leq \bar{\beta}_4(\alpha) = \frac{\alpha}{\cos^2\theta_1\cos^2\theta_2 + \alpha(1 - \cos^2\theta_1\cos^2\theta_2)} \ . \qquad (2.23)$$

$\bar{\beta}_4(\alpha)$ is a hyberbola in the $\alpha\beta$ plane and it is the divider between this region and the next, when, finally
v) $d_2 < c_1$, i. e. I_1 is to the right of I_2 and the intersection is empty. This happens when

$$\beta \geq \bar{\beta}_4 \ . \qquad (2.24)$$

We note that when $\cos^2\theta_1 = \cos^2\theta_2$ the two inner dividers, $\bar{\beta}_2$ and $\bar{\beta}_3$, both degenerate into the diagonal of the square, $\beta = \alpha$. Our findings are summarized in Fig. 1 where the five regions of the parameter space, resulting from the four dividers $\bar{\beta}_1, \ldots, \bar{\beta}_4$, are displayed for the representative values $\cos^2\theta_1 = \frac{3}{4}$ and $\cos^2\theta_2 = \frac{1}{4}$.

Next we give two illustrative examples for $k = 2$. In these examples we prescribe Π_0 by giving its eigenvectors $|\zeta_i\rangle$ and eigenvalues λ_i for the possible η interval configurations. We adopt the notation $|\zeta_i(\eta)\rangle$ $(\lambda_i(\eta))$ for the eigenvector (eigenvalue) corresponding to $\bar{q}_i(\eta) = \bar{q}_i^{opt}$.

In our first example we consider the case where ρ_1 and ρ_2 are uniformly mixed, corresponding to subspace discrimination. Then $I_1 = [c_1, d_1] \subseteq I_2 = [c_2, d_2]$, where

$$c_i = \frac{\cos^2\theta_i}{1 + \cos^2\theta_i} \ , \qquad d_i = \frac{1}{1 + \cos^2\theta_i} \ . \qquad (2.25)$$

The interval $0 \leq \eta \leq 1$ is divided into five subintervals, $[0, c_2]$, $[c_2, c_1]$, $[c_1, d_1]$, $[d_1, d_2]$, and $[d_2, 1]$. Table I summarizes the behavior of Π_0 in each of the subintervals.

For our second example we choose ρ_1 and ρ_2 so that $d_1 \leq c_2$, which can be easily arranged by picking $\beta < \bar{\beta}_1(\alpha)$. We then have intervals $[0, c_1]$, $[c_1, d_1]$, $[d_1, c_2]$, $[c_2, d_2]$, and $[d_2, 1]$. This is a situation in which the fidelity bound for the failure probability, Eq. (1.2), can never be achieved. The behavior of Π_0 is summarized in Table II.

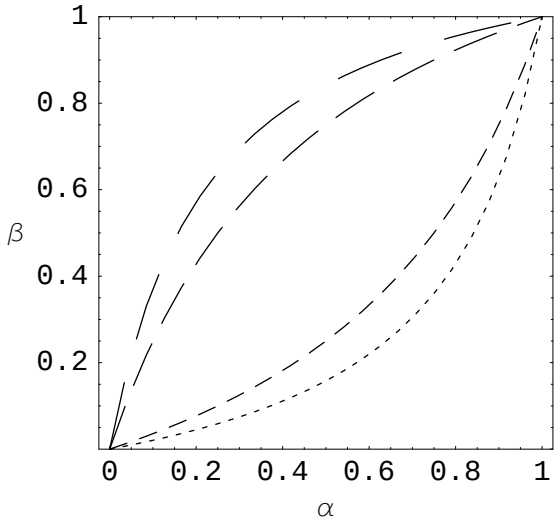

FIG. 1: Regions of the parameter space. Dotted line: $\bar{\beta}_1(\alpha)$, short dashed line: $\bar{\beta}_2(\alpha)$, medium dashed line: $\bar{\beta}_3(\alpha)$, long dashed line: $\bar{\beta}_4(\alpha)$. In the region below $\bar{\beta}_1(\alpha)$ and above $\bar{\beta}_4(\alpha)$ the intersection of I_1 and I_2 is empty, the fidelity bound can not be reached; in the regions between $\bar{\beta}_1(\alpha)$ and $\bar{\beta}_2(\alpha)$, and between $\bar{\beta}_3(\alpha)$ and $\bar{\beta}_4(\alpha)$ the intervals I_1 and I_2 partially overlap, the fidelity bound can be reached in these overlaps; and in the region between $\bar{\beta}_2(\alpha)$ and $\bar{\beta}_3(\alpha)$ the interval I_1 is inside I_2, the fidelity bound can be reached in the entire I_1. For the figure we used the values $\cos\theta_1 = \frac{\sqrt{3}}{2}$ and $\cos\theta_2 = \frac{1}{2}$.

TABLE I: Eigenvalues and eigenvectors of Π_0 in the various intervals of η for Example 1. Both states are uniformly mixed and the intersection of I_1 and I_2 is the entire I_1. The fidelity bound can be reached in the intersection.

η	λ_1	λ_2	$\|\zeta_1\rangle$	$\|\zeta_2\rangle$
$[0, c_2]$	1	1	$\|\psi_1\rangle$	$\|\psi_2\rangle$
$[c_2, c_1]$	1	$\lambda_2(\eta)$	$\|\psi_1\rangle$	$\|\zeta_2(\eta)\rangle$
$[c_1, d_1]$	$\lambda_1(\eta)$	$\lambda_2(\eta)$	$\|\zeta_1(\eta)\rangle$	$\|\zeta_2(\eta)\rangle$
$[d_1, d_2]$	1	$\lambda_2(\eta)$	$\|\psi_3\rangle$	$\|\zeta_2(\eta)\rangle$
$[d_2, 1]$	1	1	$\|\psi_3\rangle$	$\|\psi_4\rangle$

TABLE II: Eigenvalues and eigenvectors of Π_0 in the various intervals of η for the second example in the text. The intersection of I_1 and I_2 is empty and the fidelity bound cannot be reached in this case.

η	λ_1	λ_2	$\|\zeta_1\rangle$	$\|\zeta_2\rangle$
$[0, c_1]$	1	1	$\|\psi_1\rangle$	$\|\psi_2\rangle$
$[c_1, d_1]$	$\lambda_1(\eta)$	1	$\|\zeta_1(\eta)\rangle$	$\|\psi_2\rangle$
$[d_1, c_2]$	1	1	$\|\psi_3\rangle$	$\|\psi_2\rangle$
$[c_2, d_2]$	1	$\lambda_2(\eta)$	$\|\psi_3\rangle$	$\|\zeta_2(\eta)\rangle$
$[d_2, 1]$	1	1	$\|\psi_3\rangle$	$\|\psi_4\rangle$

The trend is clear from these two examples. For each of the five regions of the $\alpha\beta$ parameter plane the operating value of η can have five possibilities. It can be outside

of the intervals I_1 and I_2 (three such intervals if I_1 and I_2 do not intersect and two if they do), it can be in the nonoverlapping regions of I_1 and I_2 (two such intervals) and, finally, it can be in the intersection of I_1 and I_2 (zero or one such interval). The five parameter regions and the five possibilities for η in each of these regions give us altogether twenty five characteristically different cases. In only three of them can the fidelity bound be reached. In twelve cases the optimum measurement is a standard von Neumann projection and in the remaining ten cases it is a combination of projections in some dimensions and POVMs in the others.

We believe that these trends are general and they hold for the discrimination of any Rank 2 mixed states not just the ones where the Jordan basis coincides with the spectral representation but it will be much harder to find explicitly the different regions in the parameter space and the different intervals of the prior probability η. We also conjecture that for the discrimination of two Rank N mixed states there are $(2N+1)^N$ cases altogether and the fidelity bound can be reached in only $2N-1$ of them. Since the growth in the number of possibilities as a function of N is faster than exponential it seems as though it would be extremely difficult to give a complete classification of the cases for $N > 2$. Furthermore, since the number of cases when the fidelity bound can be reached grows only linearly with N, the weight of the density operators for which the fidelity bound can be attained quickly becomes negligible with increasing N.

III. APPLICATIONS

Let us now consider a simple example that we will be able to use as the basis for applications of subspace discrimination. Let $\mathcal{H}$ be a four-dimensional space with the orthonormal basis $\{|j\rangle \mid j = 0, \ldots, 3\}$. For the first subspace, S_1, we choose the span of the vectors $|0\rangle$ and $|1\rangle$, and for the second, S_2 we choose the span of the vectors $|u_0\rangle = (|0\rangle + |2\rangle)/\sqrt{2}$ and $|u_1\rangle = (|1\rangle + |3\rangle)/\sqrt{2}$. The states $\{|0\rangle, |1\rangle\}$ and $\{|u_0\rangle, |u_1\rangle\}$ form Jordan bases for the subspaces S_1 and S_2. Defining the vectors

$$\begin{aligned} |y_1\rangle &= |2\rangle \qquad |y_2\rangle = |3\rangle \\ |z_1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle) \qquad |z_2\rangle = \frac{1}{\sqrt{2}}(|1\rangle - |3\rangle), \end{aligned} \tag{3.1}$$

we have that $\bar{S}_1$ is the span of $|y_1\rangle$ and $|y_2\rangle$, and $\bar{S}_2$ is the span of $|z_1\rangle$ and $|z_2\rangle$. Application of the formulas in the previous section gives us the POVM for discriminating between S_1 and S_2. The POVM exists for $1/3 \leq \eta \leq 2/3$, where the detection operators are given by

$$\begin{aligned} \Pi_1 &= \sqrt{2}\left(\sqrt{2} - \sqrt{\frac{1-\eta}{\eta}}\right)\bar{P}_2 \\ \Pi_2 &= \sqrt{2}\left(\sqrt{2} - \sqrt{\frac{\eta}{1-\eta}}\right)\bar{P}_1 \ . \end{aligned} \tag{3.2}$$

The corresponding failure probability is $Q = \sqrt{2\eta(1-\eta)}$. We also mention here that this solution was already derived in [18] using a slightly less general approach.

One possible application of this POVM is the following. Suppose that Alice and Bob cannot communicate with each other, but they can communicate with Charlie. Charlie wants Alice and Bob to share a secure bit string. He sends to Alice and Bob one particle each from either of the two-particle states

$$\begin{aligned} |\Psi_0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b + |1\rangle_a|0\rangle_b) \\ |\Psi_1\rangle &= \frac{1}{\sqrt{2}}(|u_0\rangle_a|u_1\rangle_b + |u_1\rangle_a|u_0\rangle_b). \end{aligned} \tag{3.3}$$

If Alice and Bob both succeed in identifying which state was sent, they share a bit, $|\Psi_0\rangle$ corresponding to 0 and $|\Psi_1\rangle$ corresponding to 1. The reduced density matrices that Alice and Bob must distinguish are $\rho_0 = (1/2)P_1$, which results if $|\Psi_0\rangle$ is sent, and $\rho_0 = (1/2)P_2$, which results if $|\Psi_1\rangle$ is sent. The above POVM does this optimally (we shall assume that $\eta = 1/2$). The procedure would be the following. Charlie sends one of the two states to Alice and Bob (one particle to each). They independently perform their measurements. They then tell Charlie whether they succeeded, and he tells each of them whether the bit is valid or not. The bit is valid when both Alice's and Bob's measurements succeeded, and invalid otherwise.

The security comes from the fact that $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are not orthogonal. An eavesdropper, Eve, cannot perfectly distinguish these two states. Her measurement procedure will either sometimes produce errors or sometimes fail. She must, however, send particles on to Alice and Bob. There is no state she can send them that will guarantee that one or both of their measurements fail, so that sometimes Alice's and Bob's measurements will tell them that they have received a state different from the one that Charlie sent. By comparing some of their bits with those of Charlie, they can tell whether this has occurred. One possibility is that they can use some of the invalid bits, in particular the ones for which one of the measurement succeeded and the other did not. For example, if Alice's measurement succeeded, then she can tell Charlie the result of her measurement, and Charlie can see whether it corresponds to the state that he sent. If it does not, then they know that an eavesdropper was present.

A second example concerns operator discrimination [22]-[24]. Alice starts with the two-qubit state, $|\Psi_{in}\rangle = |0\rangle|0\rangle$. She sends the state through one of two black boxes, each black box performing an operation on the input state. The first black box performs an unknown, arbitrary single qubit rotation on the second qubit. The second first performs an unknown, arbitrary single qubit rotation on the second quibit and a Hadamard operation on the first, and this is followed by sending both quibits through a C-NOT gate, with the first qubit as the control and the second as the target. Alice then sends the resulting output state to Bob, who must decide which

black box Alice used. Note that what is being done here is the discrimination between two sets of operators; the first black box performs an abitrary operator from the first sent and the second black box performs an arbitrary operator from the second set.

If the input state is sent through the first black box, the output state that is sent to Bob is

$$|\Psi_{1out}\rangle = \alpha|0\rangle|0\rangle + \beta|0\rangle|1\rangle, \tag{3.4}$$

where α and β are unknown. If the input state was sent through the second black box, Bob receives the state

$$\begin{aligned} |\Psi_{2out}\rangle \;=\; & \frac{1}{\sqrt{2}}[\alpha(|0\rangle|0\rangle + |1\rangle|1\rangle) \\ & +\beta(|0\rangle|1\rangle + |1\rangle|0\rangle). \end{aligned} \tag{3.5}$$

The state $|\Psi_{1out}\rangle$ lies in the subspace spanned by the vectors $\{|0\rangle|0\rangle, |0\rangle|1\rangle\}$ and the state $|\Psi_{2out}\rangle$ lies in the space spanned by $\{(|0\rangle|0\rangle+|1\rangle|1\rangle), (|0\rangle|1\rangle+|1\rangle|0\rangle)\}$. That means that distinguishing $|\Psi_{1out}\rangle$ and $|\Psi_{2out}\rangle$ reduces to the problem of distinguishing these two supspaces. Making the correspondence with our previous example

$$\begin{aligned} |0\rangle|0\rangle &\to |0\rangle \qquad & |1\rangle|1\rangle &\to |2\rangle \\ |0\rangle|1\rangle &\to |1\rangle \qquad & |1\rangle|0\rangle &\to |3\rangle, \end{aligned} \tag{3.6}$$

we see that the problem reduces to the one we have already solved. The subspace in which $|\Psi_{1out}\rangle$ lies corresponds to S_1 and the one in which $|\Psi_{2out}\rangle$ lies corresponds to S_2. Therefore, the POVM we have already found will optimally distinguish (assuming that the input state is $|0\rangle|0\rangle$) through which black box the input state was sent.

IV. CONCLUSION

We have presented a POVM that optimally and unambiguously discriminates between two subspaces. The construction of this POVM made use of the Jordan bases of the two subspaces. The results are, in fact, more general than what is stated in the title. They represent the complete solution to the problem of optimal unambiguous discrimination between mixed states of a special class, viz. between those states for which the spectral form coincides with the Jordan representation.

We presented two applications of the measurement procedure, discriminating between two-particle states if one has only one of the particles and deciding to which of two sets an unknown quantum operation belongs.

This procedure can be used to distinguish arbitrary mixed states by discriminating between their supports, but the results will not, in general, be optimal. In order to optimally discriminate between mixed states the structure of the states within their supports must be taken into account. Based, however, on the results of this paper we believe that this is an extremely difficult task for density matrices of Rank > 2. The case of optimally discriminating between arbitrary Rank 2 density matrices appears more tractable, however. How it can be accomplished is a problem that still remains open.

Acknowledgments

This research was partially supported by a grant from PSC-CUNY as well as by a CUNY collaborative grant. JB gratefully acknowledges many helpful discussions with Ulrike Herzog (Humboldt University, Berlin), on various aspects of state discrimination.

[1] J. A. Bergou, U. Herzog, and M. Hillery, Lect. Notes Phys. **649**, 417-465 (Springer, Berlin, 2004).
[2] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[3] J. A. Bergou, U. Herzog, and M. Hillery, Phys. Rev. Lett. **90**, 257901 (2003).
[4] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[5] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[6] D. Dieks, Phys. Lett. A **126**, 303 (1988).
[7] A. Peres, Phys. Lett. A **128**, 19 (1988).
[8] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).
[9] J. A. Bergou, M. Hillery, and Y. Sun, J. Mod. Opt. **47**, 487 (2000).
[10] A. Peres and D. Terno, J. Phys. A **31**, 7105 (1995).
[11] Y. Sun, J. A. Bergou, and M. Hillery, Phys. Rev. A **64**, 022311 (2001).
[12] A. Chefles, Phys. Lett. A **239**, 339 (1998). See also A. Chefles, Contemporary Physics **41**, 401 (2000).
[13] S. Zhang and M. Ying, Phys. Rev. A **65**, 062322 (2002).
[14] Y. Sun, J. A. Bergou, and M. Hillery, Phys. Rev. A **66**, 032315 (2002).
[15] T. Rudolph, R. W. Spekkens, and P. S. Turner, Phys. Rev. A **68**, 010301(R) (2003).
[16] Y. Feng, R. Duan, and M. Ying, Phys. Rev. A **70**, 012308 (2004).
[17] P. Raynal, N. Lütkenhaus, and S. van Enk, Phys. Rev. A **68**, 022308 (2003).
[18] U. Herzog and J. A. Bergou, Phys. Rev. A **71**, 050301(R) (2005).
[19] P. Raynal and N. Lütkenhaus, quant-ph/0502165.
[20] J. A. Bergou and Mark Hillery, Phys. Rev. Lett. **94**. 160501 (2005).

[21] P. X. Gallagher and R. J. Proulx, in *Contributions to Algebra*, Bass, Cassidy, and Kovacic eds. (Academic Press, New York, 1977).
[22] A. Acin, Phys. Rev. Lett. **87**,177901 (2001).
[23] G. M. D'Ariano, P. L. Presti, and M. G. A. Paris J. Opt. B **4** 273 (2002).
[24] A. Chefles and M. Sasaki, Phys. Rev. A **67**, 032112 (2003).